

Version 10.04

Part No. NN46110-509 02.02
January 2010
Standard

600 Technology Park Drive
Billerica, MA 01821-4130

Nortel VPN Client — Configuration



Copyright © 2008–2010 Nortel Networks. All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, and Nortel VPN Router are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Entrust is a trademark of Entrust Technologies Inc.

Microsoft and Windows are trademarks of Microsoft Corporation.

Netscape and Netscape Navigator are trademarks of Netscape Communications Corporation.

SecurID is a trademark of RSA Security Inc.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. software license agreement

This Software License Agreement (“License Agreement”) is between you, the end-user (“Customer”) and Nortel Networks Corporation and its subsidiaries and affiliates (“Nortel Networks”). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

“Software” is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment (“CFE”), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer’s Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided “AS IS” without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

- a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).
- b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.
- c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.
- d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.
- e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.
- f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Preface	9
Before you begin	9
Text conventions	10
Acronyms and terms	11
Related publications	13
Hard-copy technical manuals	14
How to get help	14
Finding the latest updates on the Nortel Web site	14
Getting help from the Nortel Web site	15
Getting help over the phone from a Nortel Solutions Center	15
Getting help from a specialist by using an Express Routing Code	15
Getting help through a Nortel distributor or reseller	16
New in this release.	17
Features	17
Support	17
Client logon	19
Starting a VPN tunnel	21
Logging on using the Pre-Logon Access Provider for Windows Vista and Windows 7	22
Domain logon on XP using Two-step login	24
Viewing the Nortel VPN Client Status monitor	25
Second instance of NVC GUI	27
Client profile configuration	29
Creating an IPSec profile using the Set Up Wizard	30
Creating an IPSec profile using Manage Profiles	33
Creating a SSL profile using the Set Up Wizard	37
Creating a SSL profile using Manage Profiles	40
Creating a cloned profile	42
Editing a profile	42

Client operations configuration	45
Configuring proxy settings	46
Launching an application	47
Launching an application before connecting the NVC	47
Launching an application after connecting the NVC	47
Configuring dial-up	48
Setting Keepalives	49
Setting a Failover	49
Setting NVC management options	50
Viewing log files	51
SSL tunnel with RSA hardware token	52
Importing and obtaining digital certificates	52
Server certificate validation at client machine	53
Importing a CA certificate	53
Revocating and validating a server certificate	54
Viewing banners	56
Security banners	56
Nortel Health Agent Notify banner	56
Using the third-party API	57
Client control—Command line	59
Starting a tunnel without a profile	60
Starting a tunnel with a profile	62
Stopping a tunnel	64
Launching the NVC GUI	64
Determining tunnel status	65
Retrieving the tunnel banner	67
Retrieving command line help information	67
Retrieving NVC version information	68
Index	69

Tables

Table 1	Support	17
Table 2	NVR and NVG support	19
Table 3	NVC IPSec support	20
Table 4	NVC SSL support	20
Table 5	Configuration status information	26
Table 6	IPSec authentication information requirements	35
Table 7	SSL authentication information requirements	41
Table 8	Logging levels	51
Table 9	Third-party API files	57
Table 10	API functions	58
Table 11	Parameters for a tunnel without a profile	60
Table 12	Parameters for a tunnel with a profile	62
Table 13	Tunnel parameter for termination	64
Table 14	Parameters for launching the NVC GUI	65
Table 15	Tunnel parameters to determine status	66
Table 16	Tunnel parameter for banner	67
Table 17	Tunnel parameter for retrieving command line help information	67
Table 18	Tunnel parameter for retrieving current NVC version information	68

Preface

This guide helps you install, configure, and use the Nortel VPN Client (NVC) for the Windows XP, Windows Vista and Windows 7 operating systems. Topics include

- starting NVC
- support for NVG
- Domain logon on Vista and Windows 7 using Pre-Logon Access Provider (PLAP)
- Domain logon on XP using Two-step login
- creating profiles for IPSec and SSL tunnels
- optional configuration settings
- using the client from a script or a third-party application

This guide is intended for network managers who are responsible for setting up client software for the VPN Router. This guide assumes that you have the following background

- experience with Windows operating systems or graphical user interfaces (GUI)
- familiarity with network management

For more information about configuring and monitoring the VPN Router, see *VPN Router Configuration — Basic Features* (NN46110-500).

Before you begin

The minimum PC requirements for running the NVC are

- Windows XP, Windows Vista or Windows 7
- 1 GHz 32-bit (x86) or 64-bit (x64) processor

- 1 GB of system memory
- 40 GB hard drive with 15 GB of available space

Text conventions

This guide uses the following text conventions

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is <code>ping <ip_address></code> , you enter <code>ping 192.32.10.12</code>
bold Courier text	Indicates command names and options and text that you need to enter. Example: Use the <code>show health</code> command. Example: Enter <code>terminal paging {off on}</code> .
braces ({ })	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is <code>ldap-server source {external internal}</code> , you must enter either <code>ldap-server source external</code> or <code>ldap-server source internal</code> , but not both.
brackets ([])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is <code>show ntp [associations]</code> , you can enter either <code>show ntp</code> or <code>show ntp associations</code> . Example: If the command syntax is <code>default rsvp [token-bucket {depth rate}]</code> , you can enter <code>default rsvp</code> , <code>default rsvp token-bucket depth</code> , or <code>default rsvp token-bucket rate</code> .

ellipsis points (. . .)	<p>Indicate that you repeat the last element of the command as needed.</p> <p>Example: If the command syntax is more diskn:<i><directory>/...<file_name></i>, you enter more and the fully qualified name of the file.</p>
<i>italic text</i>	<p>Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore.</p> <p>Example: If the command syntax is ping <i><ip_address></i>, <i>ip_address</i> is one variable and you substitute one value for it.</p>
plain Courier text	<p>Indicates system output, for example, prompts and system messages.</p> <p>Example: File not found.</p>
separator (>)	<p>Shows menu paths.</p> <p>Example: Select Status > Health Check.</p>
vertical line ()	<p>Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command.</p> <p>Example: If the command syntax is terminal paging {off on}, you enter either terminal paging off or terminal paging on, but not both.</p>

Acronyms and terms

This guide uses the following acronyms and terms

API	Application Program Interface
BER	basic encoding rules
CA	Certification Authority
Certification path	Ordered sequence of certificates, leading from a certificate whose public key is known by a client to a certificate whose public key is to be validated by the client

Credential Provider	A module plug-in that handles credential information and communication with an external authentication provider
CRL	Certificate revocation list—list of revoked but unexpired certificates issued by a CA
Digital certificate	Digitally signed data structure defined in the X.509 standard that binds the identity of a certificate holder (or subject) to a public key
DLL	Dynamic Link Library
IKE	Internet Key Exchange
ISAKMP	Internet Security Association and Key Management Protocol
LDAP	Lightweight Directory Access Protocol
MSI	Microsoft Windows Installer
NVC	Nortel VPN client
NVG	Nortel VPN Gateway
PLAP	Pre-Logon Access Provider
Public Key Cryptography Standards (PKCS)	Collection of de facto standards produced by RSA covering the use and manipulation of public-private keys and certificates
PKCS #7	Cryptographic Message Standard (Reply with digital certificate)
PKCS #10	Certification Request Syntax Standard
PKCS #12	Personal Information Exchange Syntax
PKI	Public Key Infrastructure
TCP	Transmission Control Protocol
X.509	Standard certificate format

Related publications

For more information about the VPN Router, see the following publications:

- Release notes provide the latest information, including brief descriptions of the new features, problems fixed in this release, and known problems and workarounds.
- *Nortel VPN Router Configuration — Basic Features* (NN46110-500) introduces the product and provides information about initial setup and configuration.
- *Nortel VPN Router Security — Servers, Authentication, and Certificates* (NN46110-600) provides instructions for configuring authentication services and digital certificates.
- *Nortel VPN Router Security — Firewalls, Filters, NAT, and QoS* (NN46110-601) provides instructions for configuring the Stateful Firewall and VPN Router interface and tunnel filters.
- *Nortel VPN Client — Installation and Upgrades* (NN46110-412) provides instructions for installing NVC and upgrading software from previous versions.
- *Nortel VPN Router Configuration — Advanced Features* (NN46110-502) provides instructions for configuring advanced LAN and WAN settings, PPP, frame relay, PPPoE, ADSL and ATM, T1CSU/DSU, dial services and demand services, DLSw, IPX, and SSL VPN.
- *Nortel VPN Router Configuration — Tunneling Protocols* (NN46110-503) provides configuration information for the tunneling protocols IPsec, L2TP, PPTP, and L2F.
- *Nortel VPN Router Configuration — Routing* (NN46110-504) provides instructions for configuring BGP, RIP, OSPF, and VRRP, as well as instructions for configuring ECMP, routing policy services, and client address redistribution (CAR).
- *Nortel VPN Router Configuration — Troubleshooting* (NN46110-602) provides information about system administrator tasks such as backup and recovery, file management, and upgrading software, and instructions for monitoring gateway status and performance. This book also provides troubleshooting information and interoperability considerations.
- *Nortel VPN Router Using the Command Line Interface* (NN46110-507) provides syntax, descriptions, and examples for the commands that you can use from the command line interface on the VPN Router.

- *Nortel VPN Router Configuration — TunnelGuard* (NN46110-307) provides information about configuring and using the Nortel Health Agent feature.

Hard-copy technical manuals

To print selected technical manuals and release notes free, directly from the Internet, go to www.nortel.com/documentation. Find the product for which you need documentation, then locate the specific category and model or version for your hardware or software product. Use Adobe Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. For more information about a free copy of the Adobe Reader, go to the Adobe Systems Web site: www.adobe.com.

How to get help

This section explains how to get help for Nortel products and services.

Finding the latest updates on the Nortel Web site

The content of this documentation was current at the time the product was released. To check for updates to the latest documentation and software for VPN Client, click one of the following links:

Link to	Takes you directly to the
Latest software	Nortel page for VPN Client software located at: www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=SOFTWARE&resetFilter=1&poid=10621
Latest documentation	Nortel page for VPN Client documentation located at: www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=DOCUMENTATION&resetFilter=1&poid=10621

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

New in this release

The following sections details what’s new in *Nortel VPN Client — Configuration* NN46110-509 02.02 for release 10.04.

- [“Features” on page 17](#)

Features

Support

- This release provides support to the following editions of Windows XP, Windows Vista and Windows 7 operating systems.
- This release provides support for NVG.

Table 1 Support

Operating System	Edition	Single Processor		Dual Processor	
		32 bit	64 bit	32 bit	64 bit
Windows 7	Home Basic	✓	✓	✓	✓
Windows 7	Home Premium	✓	✓	✓	✓
Windows 7	Professional	✓	✓	✓	✓
Windows 7	Enterprise	✓	✓	✓	✓
Windows 7	Ultimate	✓	✓	✓	✓

Table 1 Support

Operating System	Edition	Single Processor		Dual Processor	
Vista	Home Basic	✓	✓	✓	✓
Vista	Home Premium	✓	✓	✓	✓
Vista	Business	✓	✓	✓	✓
Vista	Enterprise	✓	✓	✓	✓
Vista	Ultimate	✓	✓	✓	✓
XP	Home	✓	✓	✓	✓
XP	Professional	✓	✓	✓	✓
XP	Tablet	✓	✓	✓	✓

For more information see, [“Before you begin” on page 9](#)

Client logon

This chapter describes how you use the Nortel VPN Client (NVC) to launch a VPN tunnel using the Windows XP, Windows Vista and Windows 7 operating systems.

For information about how to install NVC and the Pre-Logon Access Provider (PLAP), and to customize installation, see *Nortel VPN Client — Installation and Upgrades* (NN46110-412).

[Table 2 “NVR and NVG support” on page 19](#) shows Nortel VPN Router (NVR) and Nortel VPN Gateway(NVG) versions that support NVC.

Table 2 NVR and NVG support

Version	NVR	NVG
10.01 and higher	version 7.xx version 8.xx	version 6.0.13 and higher version 7.xx version 8.xx

[Table 3 “NVC IPSec support” on page 20](#) shows options that are available for IPSec cipher combinations.

Table 3 NVC IPSec support

Version	IPSec cipher combination
10.01 and higher	ESP -256 AES with Sha1 ESP -128 AES with Sha1 ESP - Triple DES with SHA1 ESP - Triple DES with MD5 ESP - 56-BIT DES with SHA1 ESP - 56-BIT DES with MD5 ESP - 40-BIT DES with SHA1 ESP - 40-BIT DES with MD5 ESP - NULL with SHA1 ESP - NULL with MD5

[Table 4 “NVC SSL support” on page 20](#) shows options that are available for SSL cipher combinations.

Table 4 NVC SSL support

Version	SSL cipher combination
10.01 and higher	(DHE_RSA_WITH_3DES_EDE_CBC_SHA, 0x16) (RSA_WITH_3DES_EDE_CBC_SHA, 0x0a) (RSA_WITH_RC4_128_SHA, 0x05) (RSA_WITH_RC4_128_MD5, 0x04) (RSA_EXPORT1024_WITH_RC4_56_SHA, 0x64) (RSA_EXPORT1024_WITH_DES_CBC_SHA, 0x62) (RSA_EXPORT1024_WITH_RC4_56_MD5, 0x60) (DHE_RSA_WITH_DES_CBC_SHA, 0x15) (RSA_WITH_DES_CBC_SHA, 0x09) (DHE_RSA_EXPORT_WITH_DES40_CBC_SHA, 0x14) (RSA_EXPORT_WITH_DES40_CBC_SHA, 0x08)

This chapter includes the following topics:

- [“Starting a VPN tunnel” on page 21](#)
- [“Logging on using the Pre-Logon Access Provider for Windows Vista and Windows 7” on page 22](#)
- [“Viewing the Nortel VPN Client Status monitor” on page 25](#)

Starting a VPN tunnel

You start the VPN tunnel through a logon window. Before using NVC, you must ensure you have administrator rights to NVC to use the following functionalities

- creating global profiles
- editing, cloning and deleting options for global profiles
- clearing logs
- modifying log level settings
- Manage Option settings
 - Enable Certificate Revocation List validation for server certificate
 - Display the warning message if the VPN tunnel is still up
 - Disconnect active VPN tunnel

To use the previous functionalities, right-click the NVC.exe short cut on your desktop, and click **Run as Administrator**.

Start the NVC by performing the following procedure:

- 1 From Windows, choose **Start, All Programs, Nortel, Nortel VPN Client, Nortel VPN Client**.

The Connection window appears.

- 2 Select a connection from the **VPN Connection** list or if this your first logon, you must create a profile. For more information about creating a profile, see [“Client profile configuration” on page 29](#).
- 3 Enter a **user name** and **password** in the **Username** and **Password** fields.
- 4 Click **Connect**. A status dialog box appears showing the connection status.

After the tunnel is up, a security banner can appear depending on the NVR or NVG setting. If the security banner appears, click **Accept**. The VPN tunnel becomes fully functional. You must accept or the tunnel is taken down. Once the tunnel is fully up, a tray icon appears in the system tray.

Right-click this icon to open up an abbreviated menu. The menu lists the following options:

- Status — opens the **Status** window.
- View Log — opens the **Log Viewer** window.
- View Banner — opens the banner message for the current VPN connection.
- Configurations — opens the NVC **Manage Profiles** window. You can manage profiles and options.
- Help — opens the full Help menu for the NVC.
- About Nortel VPN Client— opens an **About** window showing NVC version information.
- Disconnect VPN — disconnects the VPN with a confirmation.

Logging on using the Pre-Logon Access Provider for Windows Vista and Windows 7

This release provides the Pre-Logon Access Provider (PLAP). A PLAP is a special type of credential provider that allows you to make a network connection before logging on to your PC.

You cannot use the Prelogon Access Provider (PLAP) functionality in conjunction with digital certificate authentication. PLAP doesn't support certificate authentication. When you attempt to make a connection, the error message Failed to connect to following reason: Authentication failure appears.

To ensure security, PLAP does not support PreLaunch and PostLaunch applications and users cannot configure profiles or other NVC settings from PLAP.

You must select Global Profile when configuring an IPSec or SSL profile to enable PLAP. For more information on configuring profiles, see [“Creating an IPSec profile using Manage Profiles” on page 33](#) and [“Creating a SSL profile using Manage Profiles” on page 40](#).

Log on the NVC with PLAP by performing the following procedure:

- 1 Log on to your PC by pressing **Ctrl+Alt+Del** to initiate the logon process. A logon window appears.

The **Ctrl+Alt+Del** keystroke sequence is called a Secure Attention Sequence (SAS). An administrator can enable or disable the SAS.

- 2 Click **Switch User** to return to the main logon window.
- 3 Click the **PLAP** icon in the lower right-hand corner of the **Nortel VPN Client** window. One of the following windows appears:

- a If a tunnel is not connected, the **Establish a VPN Connection** window appears. Go to step 4.
- b If a tunnel is connected, the **VPN Tunnel is up already** window appears. Go to step 5.

- 4 If there is not an established tunnel, you are then at the **Establish a VPN Connection** window, perform the following:

- a Click the submit button (arrow) following **Establish a VPN Connection**. The window displays the message `NVC is starting up, please wait`. This may take a few minutes then changes to `NvcGUI is still running. Waiting for it to finish up`. The **Connection** window appears.

The first time that you are attempting to launch NVC after a restart you can experience a 20 second or less delay in launching. But you can wait up until 3 minutes. If the NVC PLAP does not connect before 3 minutes, a message stating `NvcGui didn't respond. Please try again later` appears. You are then returned to the **Establish a VPN Connection** window.

Subsequent successful connections reduce the wait time after each attempt when establishing a connection.

- b Select a preconfigured global profile from the **VPN Connection** list.

- c** Type a password in the **Password** field if it is not saved, and then click **Connect**. The Connect status dialog window appears. The message VPN Tunnel has been established by NVC appears on the window and then the **main logon** window appears.

To ensure security, you cannot change the profile, make configurations, or other changes in the pre-logon stage.

- d** Log on to your PC.

You can click Disconnect beside the PLAP icon to disconnect the VPN connection as well as all other connections brought up by PLAP.

- 5** If there is an established tunnel and you are at the **VPN Tunnel is up already** window, perform the following:

- a** Click the submit button (arrow) following **VPN Tunnel is up already**. The main logon window appears.

- b** Log on to your PC.

You can click Disconnect beside the PLAP icon to disconnect the VPN connection as well as all other connections brought up by PLAP.

Domain logon on XP using Two-step login

NVC provides PLAP feature for domain logon on Vista and Windows 7 operating systems. On XP, domain logon can be achieved through "Two-Step logon" which is explained below:

- 1** User logs on to the machine using local account
- 2** Launch NVC in administrator mode
- 3** Go to **Edit the Profile** dialog and click on **Manage Options** dialog.
- 4** To set the log-off behavior, check the tab **Display the warning message if the VPN tunnel is still up**
- 5** Bring up tunnel
- 6** Manually log-off operating system. Tunnel will be maintained by NVC service component.

- 7 User logs back in using a domain account. This time, the logon authentication will be done through the tunnel with the Active Directory on the domain

Viewing the Nortel VPN Client Status monitor

The Nortel VPN Client Status monitor shows information regarding the current configuration status such as security, destination IP address, connection statistics and Keepalive parameters. Also on the window are buttons that enable you to configure and monitor the NVC.

To use the Nortel VPN Client Status monitor, perform the following:

- 1 Log on to the NVC. For more information on logons, see [“Starting a VPN tunnel” on page 21](#).
- 2 After you successfully connect to a PC over a VPN tunnel, a tray icon appears in the system tray. Clicking on the icon opens the Nortel VPN Client Status window.
- 3 View the following configuration status information on the left of the window as shown in or click on the following buttons to configure or view further information on the NVC:
 - Close — closes the status window.
 - Disconnect — disconnects the VPN with a confirmation.
 - Configuration — opens the Nortel Client Manage Profiles window. You can manage profiles and options.
 - View Banner — opens the banner message for the current VPN connection.
 - View Log — opens the Log Viewer window.
 - Help — opens the Help window.
 - About — opens an About window showing Nortel VPN Client version information.

Table 5 “Configuration status information” on page 26 lists descriptions of the NVC connection types.

Table 5 Configuration status information

Connection information	Description
Duration	Shows the current connected time for the tunnel
Security	Shows the type of security used for this tunnel
IKE	Shows the type of Diffie-Hellman cipher. Not available for SSL.
Compression	Shows the type of compression used for this tunnel
Destination IP Address	Shows the IP address of the server connecting with the NVC
Destination Port	Shows the connected port number. Not available for IPSec
Assigned IP Address	Shows the IP address assigned for this tunnel
IPSec NAT Transversal	Shows the port number of an active IPSec transmission. Not available for SSL
Logging Level	Shows the type of logging level. For more information on logging levels, see “Setting NVC management options” on page 50
Mobility	Shows the type of Mobility enabled for this tunnel
Persistence	Shows if persistent connection is enabled. Not available for SSL.
FIPS 140-2 mode	Shows the type of FIPS 140-2 encryption used for this tunnel. Not available for SSL.
Transport	Shows the type of transport used for this tunnel.
Bytes in Bytes out	Shows the number of bytes ingoing to the NVC and outgoing from the NVC
Frames in Frames out	Shows the number of frames ingoing to the NVC and outgoing from the NVC. Not available for SSL.
Encryption Decryption	Shows the number of errors occurring during encryption or decryption
Intervals Maximum retransmissions	Intervals is the number of milliseconds of wait time before sending keepalive packets Retransmissions is the time in milliseconds between retransmissions of keepalives after the Keepalive wait time expires
Always on Top	Click to keep the status monitor on top of your other programs
Details	Click to showing connection statistic details

Second instance of NVC GUI

When you launch a second instance of the NVC GUI, a status dialog box appears indicating that an active tunnel is already present on the PC.

Client profile configuration

This chapter provides information about how to configure IPsec and SSL profiles using the Set Up Wizard or with the Manage Profiles dialog box.

For information about how to install the NVC and the Pre-Logon Access Provider (PLAP), and to customize installation, see *Nortel VPN Client — Installation and Upgrades* (NN46110-412).

For information about how to configure split tunneling, mobility and persistence for use with the NVC, see *Nortel VPN Router Configuration — Basic Features* (NN46110-500).

For information about how to configure the NVC to co-exist with Microsoft IPsec Policy Service, see *Nortel VPN Router — Tunneling Protocols* (NN46110-503).

This chapter includes the following topics:

- [“Creating an IPsec profile using the Set Up Wizard” on page 30](#)
- [“Creating an IPsec profile using Manage Profiles” on page 33](#)
- [“Creating a SSL profile using the Set Up Wizard” on page 37](#)
- [“Creating a SSL profile using Manage Profiles” on page 40](#)
- [“Creating a cloned profile” on page 42](#)
- [“Editing a profile” on page 42](#)

Creating an IPSec profile using the Set Up Wizard

Use the Set Up Wizard to quickly create a standard profile on the Client.

Create a profile data file or user configuration file or machine configuration data using the Set Up Wizard, by performing the following procedure:

- 1 Choose **Start, All programs, Nortel, Nortel VPN Client, Nortel VPN Client**.

The Nortel VPN Client window appears.

- 2 From the left pane, click **Profile Wizard**.

The Nortel VPN Client Profile Wizard window appears.

- 3 Type in a profile name into the **Profile Name** box. You can also enter a description of the profile.
- 4 Click **Global Profile** if you want this profile to be viewed by all users on the operating system. You must select **Global Profile** to configure PLAP. Click **Next**.
- 5 Click **IPSec Tunnel** as a connection type for this profile. Click **Next**.
- 6 Type in an IP address or DNS for the VPN into the **Destination** box. Click **Next**.
- 7 Select one of the following Authentication types, and then click **Next**:
 - a **Username and Password**. Go to step 8.
 - b **Hardware or Software Token Card**. Go to step 9.
 - c **Digital Certificate and Smartcard**. Before using this option, you must import a certificate into the Microsoft Certificate Store. See [“Importing and obtaining digital certificates” on page 52](#). Go to step 10.
- 8 If you have selected **Username and Password**, perform the following:
 - a Type the username and password as assigned to you by the network administrator into the **Username** and **Password** boxes. Click **Next**.
 - b Click **No** if you do not have a group ID and group password. Click **Yes** if you do, and then type the group ID and group password as assigned to you by the network administrator into the **Group ID** and **Group Password** boxes. Click **Next**. Go to step 11.

The NVC does not share the group password between local computer accounts. If you log on to the local computer by using a different user account than the one you use to create the NVC profile, you must reenter the group password. For example, you log on to the local computer as the administrator, create the client profile, and log off. If you then log on to the local computer with a different user account, you must reenter the group password in the client profile. You must reenter the password regardless of how you install the Nortel VPN. Reenter the password by clicking the **Edit the Profile, Manage Profiles, <profile name>IPSec, General** tab.

- 9 If you have selected **Hardware or Software Token Card**, perform the following:
 - a Select one of the following tokens, and then click **Next**:
 - **Challenge Response Token Card**
 - **Response Only Token Card**. Click **Use Passcode** if you are using a passcode.
 - **Response Only Software Token**
 - b Type the user and token group ID, and token group password as assigned to you by the network administrator into the **User ID, Token Group ID** and **Token Group Password** boxes. Click **Next**. Go to step 11.
- 10 If you have selected **Digital Certificate and Smartcard**, perform the following:
 - a If you want to allow the NVC to select a certificate, click **Automatically select a valid certificate**. Click **Next**.
 - b If you want to manually select a certificate, select **Please select a certificate from the Microsoft Certificate Store below** to enable the Microsoft Certificate Store list. Highlight a certificate from the list. Click **Next**.
- 11 Click **No** if you do not want to dial first, and then click **Next**. Click **Yes** if you want to make a dial-up connection first. Selecting Yes opens the following section.
 - a Select a dial-up from an existing connection from the list or click **Create a new Dial-up entry**. The Set up a new dial-up connection dialog box appears.

- b** Click the **Dialing Rules** link. The Location Information dialog box appears. Enter the telephone information pertaining to your geographic area. Click **OK** to close.
 - c** Type the telephone number that the NVC uses to dial up the server into the **Telephone number** box.
 - d** Type a name that identifies the connection into the **Destination** box.
 - e** If you are using a smart card, click **Use a Smart Card**. Click **Create** if you do not want others to use this connection.
 - f** If you want all users who are using this PC to use this connection, click **Allow other people to use this connection**.
 - g** Click **Next**. The Type your user name and password section appears.
 - h** Type your user name into the **User name** box.
 - i** Type a password into the **Password** box. You can also select **Show characters** to show the password in the box and **Remember this password** to save the password without having to reenter it again.
 - j** You can optionally type a domain name into the **Domain** box.
 - k** Click **Create** to configure the new dial-up settings. Click **Next**.
- 12** Click **No** if you do not want to launch an application or **Yes** if you want to launch an application before or after your VPN connection is established. Selecting Yes opens Before and After connection sections.
 - a** In either the **Before connection** or **After connection** section, select the application you want to launch by clicking the **search** button beside the Application box. A Windows box opens from your PC. Search for and click the application executive file to enter it into the **Application** box.
 - b** Type the command line of the application into the **Command line** box.
 - c** For an application that you are starting before a connection, set a tunnel delay start up time by typing between **10** and **120** (seconds) into the **Tunnel Startup Delay** box. Click **Next**.
- 13** Select whether you will define or not define a failover profile. If you click **I will define a failover profile**, a list of previously configured profiles appears. Select a profile from this list, and then click **Next**.
- 14** Select one of the following Keepalive types then click **Next**:
 - **No Keepalives** — disables the Keepalives.

- **Active Keepalives (Dead peer detection)** — determines if a tunnel connection is available.
- **Passive Keepalives (No Dead peer detection)** — maintains state information in the local internet access device.

15 Click **Finish** to complete the creation of the profile.

Creating an IPSec profile using Manage Profiles

Create an IPSec profile, by performing the following procedure:

- 1** Choose **Start, All programs, Nortel, Nortel VPN Client, Nortel VPN Client**.

The Nortel VPN Client window appears.

- 2** From the left pane, click **Edit the Profile**.

The Manage Profiles window appears showing the General tab.

- 3** Click **New** located over the tabs. The information boxes clear to enable you to create a new profile.

- 4** From the **General** tab, choose **IPSec Tunnel** as a connection type for this profile from the **Tunnel Type** list.

- 5** Type in a profile name into the **Profile** box. You can optionally enter a description of the profile.

- 6** Click **Global Profile** if you want this profile to be viewed by all users on the operating system. You must select **Global Profile** to configure PLAP.

- 7** Type a profile name into the **Profile** box. You can optionally enter a description of the profile into the **Description** box.

- 8** Type an IP address or DNS for the VPN into the **Destination** box.

- 9** Select one of the following Authentication types:

- **Username and Password**
- **Certificate Authentication**
- **Group Security Authentication**

- 10** If you choose **Username and Password** perform the following:

- a** By default **Username and Password** is already selected. Type the username assigned to you by the network administrator into the **Username** box.
 - b** Type the password assigned to you by the network administrator into the **Password** box.
 - c** Click **Save Password** to save the password.
- 11** If you choose **Certificate Authentication** perform the following:
 - a** Click **Certificate Authentication** to enable the certificate selection.
 - b** Click **Select**. The Select a certificate window appears. Choose either step **c** or step **d**.
 - c** If you want to allow the NVC to select a certificate, click **Automatically select a valid certificate**.
 - d** If you want to manually select a certificate, select **Please select a certificate from the Microsoft Certificate Store below** to enable the Microsoft Certificate Store list. Highlight a certificate from the list.
 - e** Click **OK** to close the window.
 - f** If you want to associate an alternate name with this certificate, select a name from the **Alt Name** list. The default is None.
 - g** Click **Save** to save the new profile.
- 12** If you choose **Group Security Authentication** perform the following:
 - a** Click **Group Security Authentication** to enable the group security authentication.
 - b** Select a group authentication type from the list.
 - **Radius Authentication**
 - **Challenge Response Token**
 - **Response Only Hardware Token**
 - **Response Only Software Token**

The fields in Authentication Information area change according to the type selected. When choosing an authentication type, see [Table 6 “IPSec authentication information requirements” on page 35](#) for the required authentication information.

Table 6 IPSec authentication information requirements

Authentication type	Authentication information
Certificate	Certificate (nonmodifiable)
Radius Authentication	Username: type the username supplied by your administrator. Password: type the password supplied by your administrator. Save Password: click to save the password. Group ID: type the group identification supplied by your administrator. Group Password: type the group password supplied by your administrator.
Challenge Response Token	Username: type the username supplied by your administrator. Password: type the password supplied by your administrator. Save Password: click to save the password. Group ID: type the group identification supplied by your administrator. Group Password: type the group password supplied by your administrator.

Table 6 IPSec authentication information requirements

Authentication type	Authentication information
Response Only Hardware Token	Username: type the username supplied by your administrator. PIN: type the PIN supplied by your administrator. Save PIN: click to save the PIN. Group ID: type the group identification supplied by your administrator. Group Password: type the group password supplied by your administrator. Use Passcode: click to enable a passcode.
Response Only Software Token	Username: type the username supplied by your administrator. PIN: type the PIN supplied by your administrator. Save PIN: click to save the PIN. Group ID: type the group identification supplied by your administrator. Group Password: type the group password supplied by your administrator.

The NVC does not share the group password between local computer accounts. If you log on to the local computer by using a different user account than the one you use to create the NVC profile, you must reenter the group password. For example, you log on to the local computer as the administrator, create the client profile, and log off. If you then log on to the local computer with a different user account, you must reenter the group password in the client profile. You must reenter the password regardless of how you install the Nortel VPN.

13 Click **Save** to save the configuration.

Creating a SSL profile using the Set Up Wizard

Use the Set Up Wizard to quickly create a secure profile on the NVC.

Create a profile using the Set Up Wizard, by performing the following procedure:

- 1 Choose **Start, All programs, Nortel, Nortel VPN Client, Nortel VPN Client**.

The Nortel VPN Client window appears.

- 2 From the left pane, click **Profile Wizard**.

The Nortel VPN Client Profile Wizard window appears.

- 3 Type in a profile name into the **Profile Name** box. You can optionally enter a description of the profile.

- 4 Click **Global Profile** if you want this profile to be viewed by all users on the operating system. You must select **Global Profile** to configure PLAP. Click **Next**.

- 5 Click **SSL Tunnel** as a connection type for this profile. Click **Next**.

- 6 Type in an IP address or DNS name for the VPN into the **Destination** box. Type in the port number assigned to you by your administrator into the **Port** box. Click **Next**.

- 7 Select one of the following:

- a Click **Use certificate to authenticate** to enable the certificate selection. Click **Next**.

- b Click **Use predefined Login Service to authenticate** to enable Predefined Login Service configuration. Click **Next**.

- 8 Select one of the following Proxy settings:

- a Click **Don't Use proxy** if you don't want to apply proxy settings. This the default setting.

- b Click **Use default browser's proxy settings** if you want to use your browser proxy settings.

- c Click **Use defined proxy settings** when you want to configure your own. Clicking enables the field information.

- d** Type an IP address or DNS into the **Proxy address** box.
- e** Type the port number supplied by your administrator into the **Port** box. Click **Next**.

To exclude the IP address from being used on the proxy server, type the IP addresses into the box. Be sure to separate the addresses from each other using semicolons.

- 9** If you selected **Use certificate to authenticate** from step 7, perform the following:
 - a** If you want to allow the NVC to select a certificate, click **Automatically select a valid certificate**. Click **Next**.
 - b** If you want to manually select a certificate, select **Please select a certificate from the Microsoft Certificate Store below** to enable the Microsoft Certificate Store list. Highlight a certificate from the list, Click **Next** and then go to step 12.
- 10** If you selected **Use predefined Login Service to authenticate** from step 7, perform the following,
 - a** Select a name for the service from the **Login Service Name** list.
 - b** Click **Response Only Software Token** if you want to enable this token. Click **Next**.
 - c** Type the username as assigned to you by the network administrator into the **Username** box. Click **Next**.
- 11** Click **No** if you do not want to dial first then click **Next**. Click **Yes** if you want to make a dial-up connection first. Selecting Yes opens the following section.
 - a** Select an existing dial-up connection from the list or click **Create a new Dial-up entry**. The Set up a new dial-up connection dialog box appears.
 - b** Click the **Dialing Rules** link. The Location Information dialog box appears. Enter the telephone information pertaining to your geographic area. Click **OK** to close.
 - c** Type the telephone number that the NVC uses to dial up the server into the **Telephone number** box.
 - d** Type a name that identifies the connection into the **Destination** box.
 - e** If you are using a smart card, click **Use a Smart Card**. Click **Create** if you do not want others to use this connection.

- f** If you want all users who are using this PC to use this connection, click **Allow other people to use this connection**.
 - g** Click **Next**. The Type your user name and password section appears.
 - h** Type your user name into the **User name** box.
 - i** Type a password into the **Password** box. You can also select **Show characters** to show the password in the box.
 - j** You can optionally type a domain name into the **Domain** box.
 - k** Click **Create** to configure the new dialup settings. Click **Next**.
- 12** Click **No** if you do not want to launch an application or **Yes** if you want to launch an application before or after your VPN connection is established. Selecting Yes opens Before and After connection sections.
 - a** In either the **Before connection** or **After connection** section, select the application you want to launch by clicking the **search** button beside the **Application** box. A Windows box opens from your PC. Search for and click the application executive file to enter it into the **Application** box.
 - b** Type the command line of the application into the **Command line** box.
 - c** For an application that you are starting before a connection, set a tunnel delay start up time by typing between **10** and **120** (seconds) into the **Tunnel Startup Delay** box. Click **Next**.
- 13** Select whether you will define or not define a failover profile. If you click **I will define a failover profile**, a list of previously configured profiles appears. Select a profile from this list and then click **Next**.
- 14** Click **Finish** to complete the creation of the profile.

Creating a SSL profile using Manage Profiles

Create a SSL VPN when you are managing the security of message transmissions.

Create a SSL profile, by performing the following procedure:

- 1 Choose **Start, All programs, Nortel, Nortel VPN Client, Nortel VPN Client**.

The Nortel VPN Client window appears.

- 2 From the left pane, click **Edit the Profile**.

The Manage Profiles window appears showing the General tab.

- 3 Click **New** located over the tabs. The information boxes clear to enable you to create a new profile.

- 4 From the **General** tab, choose **SSL Tunnel** from the **Tunnel Type** list as a connection type for this profile.

- 5 Type a profile name into the **Profile** box. You can optionally enter a description of the profile into the **Description** box.

- 6 Click the **Global Profile** if you want this profile to be viewed by all users on the operating system. You must select **Global Profile** to configure PLAP.

- 7 Type an IP address or DNS for the VPN into the **Destination** box.

- 8 Type in the port number assigned to you by your Administrator into the **Port** box.

- 9 Click **Certificate Authentication** to enable the certificate selection.

- 10 Click **Select**. The Select a certificate window appears. Choose either step [a](#) or step [b](#).

- a If you want to allow the NVC to select a certificate, click **Automatically select a valid certificate**.

- b If you want to manually select a certificate, click **Please select a certificate from the Microsoft Certificate Store below** to enable the Microsoft Certificate Store list. Highlight a certificate from the list.

- 11 Click **OK** to close the window.

- 12 If you want to associate an alternate name with this certificate, select a name from the **Alt Name** list. The default is None.
- 13 Click **Predefined Login Service** to enable Predefined Login Service configuration.
- 14 Choose a name for the service from the **Login Service Name** list. See [Table 7 “SSL authentication information requirements” on page 41](#) for authentication information.
- 15 Type the username into the **Username** box.
- 16 Click **Response Only Software Token** if you want to enable this token. Type the PIN number into the **PIN** box.
- 17 Click **Save** to save the configuration.

The fields you select in the Predefined Login Service depend upon the type of Login service that you are using. When choosing an authentication type, see [Table 7 “SSL authentication information requirements” on page 41](#) for the required authentication information.

Table 7 SSL authentication information requirements

Authentication type	Authentication information
Certificate	Certificate (nonmodifiable)
Login service (second password is not required)	Username: type the username supplied by your administrator. Password: type the password supplied by your administrator. PIN: if you are using a Response Only Software token, type the PIN supplied by your administrator.
Login service (second password is required)	Username: type the username supplied by your administrator. Password: type the password supplied by your administrator. PIN: if you are using a Response Only Software token, type the PIN supplied by your administrator. Second Password: type the password supplied by your administrator.

Creating a cloned profile

You can copy a previously configured profile and then edit the information to save you time from completing all the configuration steps.

Create a cloned profile, by performing the following procedure:

- 1 Choose **Start, All programs, Nortel, Nortel VPN Client, Nortel VPN Client**.

The Nortel VPN Client window appears.

- 2 From the left pane, click **Edit the Profile**.

The Manage Profiles window appears showing the General tab.

- 3 Under the **Profile Name** found in the profile list at the top of the window, highlight the profile you want to clone.

- 4 Click **Clone**. The Clone a profile window appears. Type in a profile name and then click **OK**.

- 5 Highlight the cloned profile from the profile list and then click **Edit**. Edit the information as desired.

- 6 Click **Save** to save the configuration.

Editing a profile

Once you have a profile completed you may want to add new features to your profile, such as launching an application, or change some feature already configured, such as removing a Failover. Use the edit function to make and then enable these changes.

Edit a profile, by performing the following procedure:

- 1 Select **Start, All programs, Nortel, Nortel VPN Client, Nortel VPN Client**.

The Nortel VPN Client window appears.

- 2 From the left pane, click **Edit the Profile**.

The Manage Profiles window appears showing the General tab.

- 3 Under the **Profile Name** found in the profile list at the top of the window, highlight the profile you want to edit.
- 4 Click **Edit**. The profile information appears under the **General** tab.
- 5 Once you have edited the profile, be sure to click **Save** to save the configuration.

Client operations configuration

This chapter provides information about how to configure various Nortel VPN Client (NVC) operations such as configuring proxies, launching applications, managing options, importing certificates, and using the third-party API.

This chapter includes the following topics:

- [“Configuring proxy settings” on page 46](#)
- [“Launching an application” on page 47](#)
- [“Configuring dial-up” on page 48](#)
- [“Setting Keepalives” on page 49](#)
- [“Setting a Failover” on page 49](#)
- [“Setting NVC management options” on page 50](#)
- [“Viewing log files” on page 51](#)
- [“SSL tunnel with RSA hardware token” on page 52](#)
- [“Importing and obtaining digital certificates” on page 52](#)
- [“Viewing banners” on page 56](#)
- [“Using the third-party API” on page 57](#)

Configuring proxy settings

Using a proxy server adds security to the NVC, protecting it from unwanted access to the tunnel. You can configure the NVC to not use a proxy, use default settings, or create your own proxy.

Configure proxy settings for a profile, by performing the following procedure:

- 1 From a profile you are editing or when creating a new profile, choose **Proxy Settings** tab. The proxy setting information appears.
- 2 Click **Don't Use proxy** if you do not want to apply proxy settings. This the default setting.
- 3 Click **Use default browser's proxy settings** if you want to use your browser proxy settings.
- 4 Click **Use defined proxy settings** when you want to configure your own. Clicking enables the field information.

Note: NVC collects proxy information from Internet Explorer browser only. Based on the IE browser settings, NVC retrieves proxy information through the following methods:

- a. Automatically detects proxy using Web Proxy Autodiscovery Protocol (WPAD).
 - b. Automatically detects proxy using Proxy Auto Configuration (PAC) file specified in the browser.
 - c. Retrieves the manually configured proxy information in the browser.
- 5 Type an IP address into the **Proxy address** box.
 - 6 Type a port number into the **Port** box.

To exclude IP addresses from being used on the proxy server, type the IP addresses into the box. Be sure to separate the addresses from each other using semicolons.
 - 7 Click **Save** to save the proxy settings.

Launching an application

You can automatically launch a third party application immediately before or after connecting the NVC.

Launching an application before connecting the NVC

Launch an application before connecting the client, by performing the following procedure:

- 1 From a profile you are editing or when creating a new profile, choose the **Application Launch** tab. The application launch information appears.
- 2 In the **Before connection** section, select the application you want to launch by clicking the **search** button beside the **Application** box. A Windows box appears from your PC. Search for and click the application executive file to enter it into the **Application** box.
- 3 Type the command line of the application into the **Command line** box.
- 4 Set a tunnel delay start up time by typing between **10** and **120** (seconds) into the **Tunnel Startup Delay** box.
- 5 Click **Save** to save the configuration.

Launching an application after connecting the NVC

Launch an application after connecting the client, by performing the following procedure:

- 1 From a profile you are editing or when creating a new profile, choose the **Application Launch** tab. The application launch information appears.
- 2 In the **After connection** section, select the application you want to launch by clicking the **search** button beside the **Application** box. A Windows box appears from your PC. Search for and click the application executive file to enter it into the **Application** box.
- 3 Type the command line of the application into the **Command line** box.
- 4 Click **Save** to save the configuration.

Configuring dial-up

You can program the NVC to automatically use a dial-up connection when connecting the VPN tunnel to a server. You can create a new dial-up, as well as edit or delete an existing number from the Dialup menu.

Create a dialup, by performing the following procedure:

- 1 From a profile you are editing or when creating a new profile, choose the **Advanced** tab. The dial up information appears.
- 2 In the **Dialup** section, click on the configuration button beside the **Dialup** list box. A menu appears.
- 3 Choose **New** from the menu. The Set up a new dial-up connection dialog box appears.
- 4 Click **Dialing Rules**. The Location Information dialog box appears. Enter the telephone information pertaining to your geographic area. Click **OK** to close.
- 5 Type the telephone number that the NVC uses to dial-up the server into the **Telephone number** box.
- 6 Type a name that identifies the connection into the **Destination** box.
- 7 If you are using a smart card, click **Use a Smart Card**.
- 8 If you want all users who are using this PC to use this connection, click **Allow other people to use this connection**.
- 9 Click **Next**. The Type your user name and password section appears.
- 10 Type your user name into the **User name** box.
- 11 Type a password into the **Password** box. You can also select **Show characters** to show the password in the box and **Remember this password** to save the password without having to reenter it again.
- 12 Click **Save password** to keep this password.
- 13 You can optionally type a domain name into the **Domain** box.
- 14 Click **Create** to configure the new dial-up settings.
- 15 Click **Save** to save the configuration.

Setting Keepalives

You set Keepalives to determine if a tunnel connection is available. Because of an issue with Microsoft Windows Vista firewall, for release 10.01 and higher, passive Keepalives for all three Keepalives profiles are sent every 15 seconds from the NVC to prevent the tunnel from being brought down by the Windows operating system.

Set the Keepalive by performing the following procedure:

- 1 From a profile you are editing or when creating a new profile, choose the **Advanced** tab. The Keepalive information appears.
- 2 From the **Keepalive option** section, select one of the following Keepalive options to apply to the profile:
 - **No Keepalives** — disables the Keepalives.
 - **Active Keepalives (Dead peer detection)** — determines if a tunnel connection is available.
 - **Passive Keepalives (No Dead peer detection)** — maintains state information in the local internet access device.
- 3 Click **Save** to save the configuration.

Setting a Failover

When the Server specified in a profile cannot be reached due to various reasons. You can define a failure profile for that profile so that the client will try the failover profile whenever such a situation arises.

Set the Failover by performing the following procedure:

- 1 From a profile you are editing or when creating a new profile, choose the **Advanced** tab. The failover information appears.
- 2 From the **Failover** section, select an existing profile from the list to use as the Failover.
- 3 Click **Save** to save the configuration.

Setting NVC management options

Use the management options when setting the level of information for log files or to program responses to VPN disconnections.

Set NVC options by performing the following procedure:

- 1 Choose **Start, All programs, Nortel, Nortel VPN Client, Nortel VPN Client**.

The Nortel VPN Client window appears.

- 2 From the left pane, click **Edit the Profile**.

The Manage Profiles window appears showing the General tab.

- 3 From the left pane, click **Manage Options**.

The Manage Options window appears.

- 4 Choose from the following list of options, and then click the box to enable the option:

- Disconnect dialup connection when VPN is disconnected — the NVC disconnects the dial-up connection when the VPN is disconnected. By default, the dial-up connection is left on.
- Enable Certificate Revocation List validation for server certificate — checks for certificates that have been revoked or are no longer valid.
- Send unencrypted packets to debugger — when enabled, unencrypted packets are sent to system debugger in hex format. The user can use DbgView or other tools to catch and display them. By default, this option is turned off.
- When I Log off from Windows — enabled by default, the Display the warning message if the VPN tunnel is still up warning message allows you the ability to log off while keeping an active connection. Selecting Disconnect active VPN tunnel removes the warning message and disconnects the tunnel when you log off of Windows.
- Logging Level — select a level to view when using the Log Viewer. Default level is Informational.

Use the information in [Table 8 “Logging levels” on page 51](#) when choosing a logging level .

Table 8 Logging levels

Logging level	Description
Debug	Shows detailed information to help you to debug a problem. Also logs positive events that mark successful milestones.
Information	Shows general type (high level) of information. Logs important and successful milestones of application execution, regardless of whether the application is working properly or not.
Warning	Shows a possible problem has occurred or can occur, but the application still functions correctly. However, it cannot continue to work properly.
Error	Shows that unexpected processing has happened. The application cannot perform a task as expected. However, the application is still up and running.
Fatal	Shows unhandled exceptions where the application has stopped working.
Disabled	The logging level is disabled. No logs are generated.

5 Click **Apply** to save the option.

Viewing log files

Use log files generated by the NVC when determining problems or monitoring the health of a connection. To set the level of a log, go to [“Setting NVC management options” on page 50](#).

View a log file by performing the following procedure:

- 1** Choose **Start, All programs, Nortel, Nortel VPN Client, Nortel VPN Client**.

The Nortel VPN Client window appears.

- 2** From the left pane, click **View Logs**. The Log information window opens.
- 3** If you want to export a log, click **Export** and then select a folder to save the file.

- 4 Click **Clear** to clear the log or **Refresh** to update the current log.

SSL tunnel with RSA hardware token

You can bring up the SSL tunnel using RSA hardware token as the authentication mechanism.

Perform the following procedure to bring up the SSL tunnel with RSA hardware token.

- 1 Launch NVC.
- 2 Click **Edit the Profile**.
- 3 Create SSL profile with authentication type **Predefined Login service**.
- 4 Name the SSL profile as **ssl_rsa_hw_token**.
- 5 In the **IP Address** field, specify the server IP address.
- 6 Click **Refresh** and select **Login service** corresponding to RSA authentication.
- 7 Type the username.
- 8 Click **Save** to save the profile.
- 9 Close the *Edit the Profile* window.
- 10 Select the profile *ssl rsa hw token* from the main window.
- 11 Type the passcode in the password field.
- 12 Click **Connect**.

Note: To get the passcode, append the token number to the pin. For example, if pin is **1234** and token is **55667788**, then passcode is **123455667788**.

Importing and obtaining digital certificates

The NVC supports retrieval of X.509v3 certificates from Microsoft Certificate storage through the Microsoft CryptoAPI (MS CAPI). Microsoft provides a Public Key Infrastructure (PKI) that adheres to the Public-Key Cryptography Standards (PKCS).

You need to import certificates into Personal store of your account. NVC lists all the certificates installed in the Personal store so that you can select a specified certificate while creating a profile.

NVC interacts only with Microsoft certificate store. The smart card vendor software copies certificates available in smart card to the Microsoft certificate store. Once the certificates are copied to Microsoft certificate store, NVC retrieves those certificates using Microsoft CryptoAPI (MS CAPI).

Server certificate validation at client machine

As part of SSL handshake between client and VPN server, VPN server sends a digital certificate to client machine. NVC validates this server certificate received at client machine. In order to validate the server certificate, NVC requires CA certificate of the server certificate under Trusted Root Certification Authority of your account. Windows operating system comes with all well known CA certificates in its MS-CAPI store.

If you try to bring up SSL tunnel through PLAP, CA certificate of server certificate must be available under Trusted Root Certification Authority of computer account. You can create certificate requests with tools that a Certification Authority (CA) supports and are integrated with MS CAPI.

If server certificate is involved in bringing up IPsec tunnels, you need to import CA certificate of server certificate under Trusted Root Certification Authority of your account. If you are trying to bring up tunnel through PLAP, CA certificate of certificate must be available under the Trusted Root Certification Authority of computer account.

Importing a CA certificate

You can import a CA certificate by performing the following procedure:

- 1 Choose **Start, Run**.
- 2 Type **mmc.exe**.
- 3 Press **ENTER**.
- 4 Choose **Add/Remove Snap-in** from the **File** menu.

The Add/Remove Snap-in window opens.

5 Click **Add**.

The Add Standalone Snap-in window appears.

6 Select **Certificates**.

7 Click **Add**.

The Certificates Snap-in window appears.

8 Select **My user account** or **Computer account**.

9 Click **Finish**.

10 Close the **Add Standalone Snap-in** window.

11 Click **OK** to close the Add/Remove Snap-in window.

12 In the **Console Root** window, right click on **Trusted Root Certification Authorities**.

13 Select **All Task, Import**.

Revocating and validating a server certificate

In the Manage options window, if the **Enable Certificate Revocation List Validation for server certificate** option is checked, then the NVC verifies the server certificate revocation status. Check the CRL database of the certificate authority to perform the server certificate verification. The locations of CRL database are available in the CRL Distribution points field of the certificate.

CRL distribution points must be reachable to the client machine before bringing up the SSL tunnel. You cannot bring up the SSL tunnel if CRL link is inaccessible or server certificate is revoked.

On the other hand, to bring up the IPsec tunnel, the CRL distribution points need to be accessible only after tunnel connection is completed. Once the IPsec tunnel is up, NVC checks the CRL status of server certificate. If NVC detects that server certificate is revoked or CRL Distribution Points are inaccessible, it tears down the tunnel.

For more information about certificate selections after they are in the MS CAPI, see [“Creating an IPSec profile using Manage Profiles” on page 33](#) or [“Creating a SSL profile using Manage Profiles” on page 40](#).

Viewing banners

Banners display security and notification messages. You can receive one of the following types of banner messages:

- security banners
- Nortel Health Agent notify banners

To view a banner, click the Nortel VPN Client icon in the system tray, and choose **View Banners**.

Security banners

A security banner displays a message that is pushed from the server when a VPN tunnel is established, if the banner is configured on the server. All traffic to the server is blocked until the user acknowledges the banner. You have three options:

- Accept/Close — allows traffic to flow and the dialog box closes
- Accept — allows traffic to flow, the security banner remains visible, and all links are clickable
- Cancel — terminates the tunnel immediately

If you enable Dynamic Domain Name System (DNS) at the group level on the server, the DNS registration to the assigned DNS server occurs after you accept the security banner.

The security banner has a timeout. If you do not do anything, the connection terminates after two minutes.

Nortel Health Agent Notify banner

If Nortel Health Agent checking is enabled on the server, the server periodically checks for the existence of Nortel Health Agent. If this check fails, the server sends a message to the NVC. The contents of the message displays in a message box.

For more information about this banner, see *Nortel VPN Router Configuration—TunnelGuard* (NN46110-307).

Using the third-party API

The third-party API provides you with the ability to start, monitor and stop VPN tunnels under a C/C++ program's control.

In this release you can use API on Windows XP, Windows Vista and Windows 7 through both 32-bit and 64-bit systems. The 10.01 version and higher's API is not backward compatible with earlier versions of API.

[Table 9 “Third-party API files” on page 57](#) lists third-party API 32-bit and 64-bit files.

Table 9 Third-party API files

32-bit	64-bit	Description
NvcApi.h	NvcApi.h	Defines the functions of the .dll files
NvcApi32.lib	NvcApi64.lib	Library file
NvcApi32.dll	NvcApi64.dll	Contains the functions.

You can use the following work flow whenever you are working with a third-party API:

- 1 Start a VPN tunnel with NVCStart (LPWSTR commandline).
- 2 Monitor the tunnel by polling NVCTunnelStatus() while performing whatever other work is required.
- 3 Stop the VPN tunnel with NVCStop().

Use the following information in [Table 10 “API functions” on page 58](#) found in the NvcApi.h file to help you use the third-party API.

Table 10 API functions

Function	Synopsis	Arguments	Returns
NVCStart(LPWSTR commandline)	Start a VPN tunnel using the nvc.exe client.	Long Pointer to Wide String (LPWSTR) commandline — A null-terminated string with the command line options for nvc.exe. Do not type the program name, for example, nvc.exe. Type only the command switches.	0 — Successfully started tunnel. -1 — Error starting nvc.exe. other — Error starting tunnel. Error code can be interpreted by NVCGetErrorString()
NVCStop ()	Stops the VPN tunnel.	None	-1 — NVC is not running. 0 — Success, stop command is issued.
NVCTunnelStatus ()	Returns the current status of the VPN tunnel.	None	-1 — NVC is not running. 0 — Tunnel is DOWN. 1 — Tunnel is UP.
NVCTunnelStats (NVC_TUNNELSTATS *statsBuffer)	Returns the tunnel current statistics.	statsBuffer — Points to a NVC_TUNNELSTATS structure that contains the current statistics. The GetSystemTime() is the UTC time when the system collects statistics. The total items are total numbers of bytes and errors the VPN driver processes from the VPN start time. (total for all tunnels). The conn items are the totals for the latest tunnel connection. These items are mirrored in the Nortel VPN Client monitor.	0 — Success other — A Microsoft Window's RPC_STATUS code.
NVCGetErrorString (int errorCode LPWSTR errorString DWORD len)	Converts an error code returned by NVCStart() to a readable string.	int errorCode — The error code returned by NVCStart(). LPWSTR errorString — A character buffer where the error string is written upon successful completion of this call. DWORD len — The length, in bytes, of the errorString buffer.	Positive value — Success with string length. 0 — String not available.

Client control—Command line

This chapter tells you how to configure and control the Nortel VPN Client (NVC) using DOS command lines instead of using the NVC GUI. You can create a profile, start and stop the NVC, as well as retrieving Help and banner information.

This chapter includes the following topics:

- [“Starting a tunnel without a profile” on page 60](#)
- [“Starting a tunnel with a profile” on page 62](#)
- [“Launching the NVC GUI” on page 64](#)
- [“Stopping a tunnel” on page 64](#)
- [“Determining tunnel status” on page 65](#)
- [“Retrieving the tunnel banner” on page 67](#)
- [“Retrieving command line help information” on page 67](#)
- [“Retrieving NVC version information” on page 68](#)

Starting a tunnel without a profile

You can configure IPsec and SSL tunnels without profiles when you want to create a tunnel to connect to a VPN server.

To configure an IPsec tunnel without a profile, enter the following command:

```
nvc.exe {-ipsec} {-auth <authentication type>} {-serverip <server ip>} {-user <username>} [-pwd <password>] [-pwd2 <password2>] [-gid <gid>] [-gpwd <group password>] [-pin <PIN>] [-code <tokenCode>] [-altname <subj-alt-name>] [-alttype <number>] [-s] [-fs] [-hidetrayicon]
```

Use the information in [Table 11 “Parameters for a tunnel without a profile” on page 60](#) to configure an IPsec tunnel.

To configure a SSL tunnel without a profile, enter the following command:

```
nvc.exe {-ssl} {-auth <authentication type>} {serverip <server ip>} {-serverport <server port>} [-proxyip <proxy ip>] [-proxyport <proxy port>] [-usebrowserproxy] [-loginservice <loginservice name>] {-user <username>} [-pwd <password>] [-pwd2 <password2>] [-pin <PIN>] [-code <tokenCode>] [-altname <subj-alt-name>] [-alttype <number>] [-s] [-fs] [-hidetrayicon]
```

Use the information in [Table 11 “Parameters for a tunnel without a profile” on page 60](#) to configure a SSL tunnel.

Table 11 Parameters for a tunnel without a profile

Switch	Value	Description
-ipsec -ssl	none	Optionally selects the tunnel type. If either type is not stated, IPsec is the default.
-profile -userProfile	Profile name	Specifies an optional preconfigured profile to use. -profile indicates a public profile to load. -userProfile indicates a private or user profile to load.
-auth	0 or userpass	Public or private logon
	1 or challenge	Challenge or response token card.
	2 or securid	SecurId hardware token.
	3 or grouppass	Simple group ID, password with username, or password.

Table 11 Parameters for a tunnel without a profile

Switch	Value	Description
	4 or challengeswtoken	Challenge or response software token.
	5 or softid	SecurID software token.
	6 or loginservice	Login Service name for SSL tunnel
	9 or mscapi	MSCAPI certificate.
	10 or profile	Authentication type comes from the specified profile.
-serverip	Server name or IP address.	Server name or IP address.
-serverport	Server port for ssl connection	Server port number for the SSL tunnel.
-proxyip	Proxy IP address	Proxy IP address.
-proxyport	Proxy port	Port number of the proxy server.
-usebrowserproxy	None	Collects proxy information from the browser.
-loginservice	Login service name	Login service name for SSL tunnel.
-user	User name	Username supplied by an administrator.
-pwd	Password	Password supplied by an administrator.
-pwd2	Password2	Second password for SSL tunnel.
-gid	Group ID	Group ID supplied by an administrator.
-gpwd	Group password	Group password supplied by an administrator.
-pin	PIN	PIN supplied by an administrator when you use Response Only Hardware Token or Response Only Software Token.
-code	Token code	SecurID uses the token code.
-altname	Certificate — alternate name	An alternate name of the certificate.
-alttype	Certificate — alternate type	Alternate type of the certificate.
-s	None	Run in full silent mode, where all popups are suppressed, including the error messages,
-fs	None	Run in full silent mode, where all popups are suppressed, including the error messages, as well as displaying the banner. If -s and -fs occurs together, then -fs overrides -s.
-hidetrayicon	None	Hides the system tray.

Starting a tunnel with a profile

You can configure IPSec and SSL tunnels with a profile when you want to create a tunnel to connect to a VPN server. Parameters required for the tunnel creation are collected from the profile name specified in the command line switch. At the same time, you have the option to override parameters available in the profile by using command line switches. You cannot override the tunnel type and authentication type in profile based tunnels.

To configure a tunnel with a profile, enter the following command:

```
nvc.exe {-profile <profile name> | -userprofile <profile name>}
{-auth <authentication type>} [-serverip <server ip>] [-user
<username>] [-pwd <password>] [-pwd2 <password2>] [-gid <gid>]
[-gpwd <group password>] [-pin <PIN>] [-code <tokenCode>] [-altname
<subj-alt-name>] [-alttype <number>] [-s] [-fs] [-hidetrayicon]
```

Use the information in [Table 12 “Parameters for a tunnel with a profile” on page 62](#) to tunnel with a profile.

Table 12 Parameters for a tunnel with a profile

Switch	Value	Description
-profile -userProfile	Profile name	Specifies an optional pre-configured profile to use. -profile indicates a public profile to load. -userProfile indicates a private or user profile to load.
-auth	0 or userpass	Public, private logon.
	1 or challenge	Challenge or response token card.
	2 or securid	SecurId hardware token.
	3 or grouppass	Simple group ID, password with username, password.
	4 or challengeswtoken	Challenge or response software token.
	5 or softid	SecurID software token.
	6 or loginservice	Login Service name for SSL tunnel.
	9 or mscapi	MSCAPI certificate.
	10 or profile	Authentication type comes from the specified profile.
-serverip	Server name or IP address.	Server name or IP address.
-user	User name	Username supplied by an administrator.

Table 12 Parameters for a tunnel with a profile

Switch	Value	Description
-pwd	Password	Password supplied by an administrator.
-pwd2	Password2	Second password for SSL tunnel.
-gid	Group ID	Group ID supplied by an administrator.
-gpwd	Group password	Group password supplied by an administrator.
-pin	PIN	PIN supplied by an administrator when you use Response Only Hardware Token or Response Only Software Token.
-code	Token code	SecurID uses the token code.
-altname	Certificate — alternate name	An alternate name of the certificate.
-alttype	Certificate — alternate type	Alternate type of the certificate.
-s	None	Run in full silent mode, where all popups are suppressed, including the error messages,
-fs	None	Run in full silent mode, where all popups are suppressed, including the error messages, as well as displaying the banner. If -s and -fs occurs together, then -fs overrides -s.
-hidetrayicon	None	Hides the system tray.

Stopping a tunnel

You use the stop tunnel command to disconnect the current tunnel.

To stop a tunnel, use the following command:

```
nvc.exe {-t|-terminate}
```

Use the information in [Table 13 “Tunnel parameter for termination” on page 64](#) to terminate the tunnel.

Table 13 Tunnel parameter for termination

Switch	Value	Description
-terminate -t	None	Terminate current tunnel.

Launching the NVC GUI

You can use the command line to launch the NVC GUI as well as to launch it with a specific profile.

To launch the NVC GUI, enter the following command:

```
nvc.exe
```

To launch the NVC GUI with a profile, enter the following command:

```
nvc.exe {-userprofile <profile name> |-profile <profile name>} [-s]  
[-fs] [-hidetrayicon]
```


Use the information in [Table 14 “Parameters for launching the NVC GUI”](#) on [page 65](#) to launch the NVC GUI.

Table 14 Parameters for launching the NVC GUI

Switch	Value	Description
-profile -userProfile	Profile name	Specifies an optional preconfigured profile to use. -profile indicates a public profile to load. -userProfile indicates a private or user profile to load.
-s	None	Run in full silent mode, where all popups are suppressed, including the error messages,
-fs	None	Run in full silent mode, where all popups are suppressed, including the error messages, as well as displaying the banner. If -s and -fs occurs together, then -fs overrides -s.
-hidetrayicon	None	Hides the system tray.

Determining tunnel status

Use the tunnel status command whenever you need to view statistics about the state of the tunnel that you are currently using.

To determine the state of a tunnel status, enter the following command:

```
nvc.exe {-status}[-details][-stats]
```

Use the information in [Table 15 “Tunnel parameters to determine status”](#) on [page 66](#) to determine the status of the tunnel.

Table 15 Tunnel parameters to determine status

Switch	Value	Description
-status	None	Gives the current tunnel status — Active or No Tunnel found
-details	None	<p>Lists the following details about the tunnel:</p> <ul style="list-style-type: none">• Security — type of encryption and hash• IKE — version of Diffie-Helen group• Compression — type of compression• Destination IP Address• Assigned IP Address• IPsec NAT Traversal — active or inactive• Logging — level of logging or disabled• Mobility — enabled or disabled• Persistence— enabled or disabled• FIPS 140-2 Mode — type of mode or disabled• Keepalive Interval — milliseconds of wait time before sending keepalive packets• Maximum retransmissions — milliseconds of time between retransmissions of Keepalives after the keepalive wait time expires
-stats	None	<p>Lists the following tunnel statistics:</p> <ul style="list-style-type: none">• Tunnel active — active or no tunnel found• Duration — time the tunnel has been active• Bytes in — number of bytes entering in to the NVC• Frames in — number of frames entering in to the NVC• Bytes out — number of bytes going out of the NVC• Frames out — number of frame going out of the NVCt• Errors — number of errors.

Retrieving the tunnel banner

View the tunnel banner on the tunnel.

To retrieve the tunnel banner, enter the following command:

```
nvc.exe {-banner}
```

Use the information in [Table 16 “Tunnel parameter for banner” on page 67](#) to retrieve the tunnel banner.

Table 16 Tunnel parameter for banner

Switch	Value	Description
-banner		Retrieves tunnel banner.

Retrieving command line help information

Use the retrieve command line help information command whenever you need to access the help.

To retrieve command line help information, enter the following command:

```
nvc.exe {-h|-help}
```

Use the information in [Table 17 “Tunnel parameter for retrieving command line help information” on page 67](#) to retrieve command line help information.

Table 17 Tunnel parameter for retrieving command line help information

Switch	Value	Description
-h -help		Retrieves the command line help information.

Retrieving NVC version information

You need to know the current version of the NVC whenever you are upgrading to avoid possible software conflicts.

To retrieve the current NVC version information, enter the following command:

```
nvc.exe {-v|-version}
```

Use the information in [Table 18 “Tunnel parameter for retrieving current NVC version information” on page 68](#) to retrieve the current NVC version.

Table 18 Tunnel parameter for retrieving current NVC version information

Switch	Value	Description
-version		Retrieves the client version information

Index

C

[Cloned profile 42](#)

D

[Dial-up 48](#)

[Digital certificates 52](#)

DOS

[Help information 67](#)

[Launching the NVC GUI 64](#)

[NVC version 68](#)

[Start a tunnel 60](#)

[Start a tunnel with profile 62](#)

[Start a tunnel without profile 60](#)

[Stop a tunnel 64](#)

[Tunnel Banner 67](#)

[Tunnel status 65](#)

F

[Failover 49](#)

I

[IPsec profile 30](#)

K

[Keepalives 49](#)

L

[Launching an application 47](#)

[Log files 51](#)

[Logon 19](#)

M

[Manage Options 49, 50](#)

P

[PLAP 22](#)

[Proxy 46](#)

[publications](#)

[hard copy 14](#)

S

[security banner 56](#)

[SSL profile 40](#)

T

[technical publications 14](#)

[Third-party API 57](#)